UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF WASHINGTON

ERWIN EYKEL, individually and on behalf of all others similarly situated, Plaintiff, v. PREMERA BLUE CROSS, a Washington Corporation, Defendants.	Case No.: **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

BADGLEY MULLINS TURNER PLLC
19929 Ballinger Way NE, Suite 200
Shoreline, WA 98155
Tel:(206) 621-6566 Fax: (206) 621-9686

TABLE OF CONTENTS

BADGLEY MULLINS TURNER PLLC
19929 Ballinger Way NE, Suite 200
Shoreline, WA 98155
Tel:(206) 621-6566 Fax: (206) 621-9686

BADGLEY MULLINS TURNER PLLC
19929 Ballinger Way NE, Suite 200
Shoreline, WA 98155
Tel:(206) 621-6566 Fax: (206) 621-9686

This is a lawsuit against Premera Blue Cross, a Washington Corporation ("Premera" or "Defendant"), a healthcare insurer which uses computer systems to store highly sensitive an highly confidential information about current and former customers and employees, including Social Security numbers ("SSNs"), names, addresses, dates of birth, medical records and financial information, which they are required and duty bound to safeguard from unauthorized disclosure and theft. The Plaintiff Erwin Eykel, seeks remedies on behalf of himself individually and on behalf of a Nationwide Class and subclass, as defined below, arising from Defendant's failure to adhere to its duties and responsibilities resulting in, and associated with, a data breach affecting several million past and present customers, employees and individuals that received treatment from Premera doctors for which they were insured by other healthcare carriers and Defendant's failure to ***immediately*** and ***accurately*** notify all interested parties to prevent them from becoming victims of or otherwise being damaged by identity theft. The facts and information alleged herein are based upon an investigation by counsel. Plaintiff believes that further substantial evidentiary support for the allegations herein will exist after a reasonable opportunity for further investigation and discovery. In support of this Complaint against Premera, Plaintiff alleges on information and belief:

I. INTRODUCTION

1. The increasing frequency of cyber-attacks on the healthcare and health insurance industries is a matter of considerable concern and importance. Ponemon Institute, an independent cyber security research institution, has recently reported that approximately ninety percent of healthcare organizations have confessed that they have been the victims of at least one data breach in the last two years. It has also been reported by Identity Theft Research Center that the medical and healthcare industry accounted for approximately 42.5% of all data breaches throughout the nation in 2014.[1]

[1] *See* Ponemon Institute LLC, Fourth Annual Benchmark Study on Patient Privacy & Data Security 2 (Mar. 2014), http://www.ponemon.org/local/upload/file/ID%20ExpertsPatient%20Privacy%20%26%20Data%20Security%20Report%20FINAL1-1.pdf. Identity Theft Resource Center, Data Breach Reports (Dec. 31, 2014), http://www.idtheftcenter.org/images/breach/DataBreachReports_2014.pdf.

BADGLEY MULLINS TURNER PLLC
19929 Ballinger Way NE, Suite 200
Shoreline, WA 98155
T: 206-621-6566
F: 206-621-9686

2. Healthcare industry companies like Premera well know of the risk of cyber attack. It is imperative that healthcare and health insurance companies assume a corresponding duty to guard against these known and anticipated risks and prevent future attacks.

3. Despite knowing of the considerable risk of cyber attack and although in 2014 the United States Federal Bureau of Investigation warned the healthcare industry about an increasing risk of such attacks, Defendant Premera failed to fulfill its legal duty to protect the sensitive and confidential information of its customers and patients receiving care from Premera healthcare providers, including Plaintiff. Premera is one of the larger healthcare insurance companies in the Pacific Northwest region with approximately two million individuals insured in Washington and Alaska alone. It has been a major provider to several large publicly traded companies including Starbucks, Microsoft, and Amazon. Premera knew that the data it collected and stored constituted highly sensitive personal and health information and that it bore the crucial responsibility to protect this information from compromise and theft.

4. On March 17, 2015, Premera disclosed that its systems had been hacked compromising and exposing the personal and healthcare information of approximately eleven million past and current policy holders. Plaintiff was provided notice of this breach by letter dated March 17, 2015:

> Our investigation determined that the attackers may have gained unauthorized access to your information, which could include your name, address, telephone number, date of birth, Social Security number, member identification number, bank account information, email address if provided to us, and claims information, including clinical information.

5. Premera has disclosed that hackers gained access to customer names, addresses, dates of birth, email addresses, telephone numbers, Social Security numbers, member identification numbers, bank account information and claims information, including personal claim data.

6. Compounding the harm caused by Premera, it has now been disclosed that the Company knew about the data breach of its system over six weeks before publicly disclosing the breach. Premera first learned its system was compromised on January 29, 2015, but did

BADGLEY MULLINS TURNER PLLC
19929 Ballinger Way NE, Suite 200
Shoreline, WA 98155
T: 206-621-6566
F: 206-621-9686

nothing to warn its customers for approximately six weeks. Worst yet, the Premera breach occurred only weeks after federal auditors had explicitly warned Premera that its security systems were inadequate and could be exploited.

7. The cyber security attack inflicted upon Premera and the consequent theft of confidential and highly sensitive information is the direct and proximate result of Defendant's failure to adequately implement cyber security measures under the fiduciary duties it has undertaken because it is a storehouse of vast quantities of sensitive customer data of individuals who have no choice but to provide that data to Premera and its healthcare systems providers to receive their services.

8. To date, Premera has not fully and accurately informed those affected of the precise scope of the theft or the nature of the risk of identity theft. While the Plaintiff has been notified, it remains unclear how many other victims the Company has notified. Premera estimates that the notification process will be complete on April 20, 2015. In a data breach situation, it is essential and incumbent upon the breached company to provide accurate and complete information to those at risk so they may immediately protect themselves and their families from further harm. In addition, The Health Insurance Portability and Accountability Act ("HIPAA") requires that Premera Blue Cross provide notice without unreasonable delay and no later than sixty days after discovery of a breach. *See* 45 C.F.R. §164.404. Washington state law requires Premera to provide notice in the most expedient time possible. *See* RCW 19.255.010.

9. Because of Premera's breach of its duties and other violations in failing to adequately safeguard and protect the sensitive information in its possession, custody and control from breach, is that Plaintiff and members of the Class shall henceforth live in fear of identity theft caused by Premera's profound lack of data security systems and controls and shall be required to expend monies to protect themselves from identity theft, albeit perhaps much too late, given Premera's misfeasance compounded by its untimely notice.

//

//

BADGLEY MULLINS TURNER PLLC
19929 Ballinger Way NE, Suite 200
Shoreline, WA 98155
T: 206-621-6566
F: 206-621-9686

II. PARTIES

10. Plaintiff Erwin Eykel is a domiciliary and resident of Seattle, WA. Mr. Eykel was insured under a Premera Blue Cross policy from January 1, 2003 to October 31, 2011. Mr. Eykel has suffered harm because his personal and health information was compromised when the cyber security systems of Premera Blue Cross were breached beginning in and around May 5, 2014, and he has spent and will spend time and money safeguarding himself from this cyber attack.

11. Premera is a Washington Corporation registered with the Washington Secretary of State to do business in Washington. Premera's headquarters is located at 7001 220th Street SW, Mount Lake Terrace, Washington 98043. Premera also maintains offices and operations in Seattle and Spokane, Washington.

12. Premera provides healthcare benefits in Alaska as Premera Blue Cross/Blue Shield of Alaska. It has registered with the Alaska Secretary of State to do business in Alaska. Defendant Premera and Defendant Premera Blue Cross/Blue Shield of Alaska are independent licensees of the Blue Cross/Blue Shield Association.

13. Premera is a health insurance provider that offers comprehensive life, vision, dental, stop-loss disability, and work force wellness service to over 1.8 million current members in Washington and Alaska. Its fiscal year 2013 revenues were $7.6 billion. In Washington and Alaska, Premera maintains a network of over twenty-seven thousand healthcare professionals.

14. Premera also maintains several affiliates that are not licensees of the Blue Cross/Blue Shield Association. These affiliates include LifeWise Health Plan of Oregon; LifeWise Health Plan of Washington; LifeWise Insurance Company; Conexion Insurance Solutions, Inc.; and Vivacity. In addition those who were insured with other Blue Cross/Blue Shield affiliates may receive health care services from a doctor, hospital or other healthcare provider who filed a claim with Premera. Individuals who had health plan benefits offered directly by Blue Cross/Blue Shield affiliates, may have had their personal data and information exposed because Premera helped process health plan claims whenever such individuals received healthcare services in the states where Premera operates.

BADGLEY MULLINS TURNER PLLC
19929 Ballinger Way NE, Suite 200
Shoreline, WA 98155
T: 206-621-6566
F: 206-621-9686

15. Premera's affiliates maintain 1.9 million members in Washington, Alaska and Oregon and reported consolidated fiscal year 2013 revenue of $3.36 billion. In addition, Premera's data systems store the personal and confidential information and medical records of many more individuals insured with a different health plan but had claims processed by Premera by having received health care services in Washington or Alaska where Premera operates.

16. Premera, Premera Blue Cross & Blue Shield of Alaska and its affiliates are collectively referred to in this Complaint as "Premera."

III. JURISDICTION AND VENUE

17. Jurisdiction is proper in this Court under the Class Action Fairness Act, 28 U.S.C. § 1332(d), because members of the proposed Plaintiff Class are citizens of states different from Defendant's home state, and the aggregate amount in controversy exceeds in $5,000,000, exclusive of interests and costs.

18. This Court has personal jurisdiction over Premera because Premera is licensed to do business in Washington, regularly conducts business in Washington, and has minimum contacts with Washington.

19. Venue is proper in this Court under 28 U.S.C. § 1391(a) because Premera regularly conducts business and resides in this district, a substantial part of the events or omissions giving rise to these claims occurred in this district, and Premera has caused harm to Class members residing in this district.

IV. FACTUAL BACKGROUND

A. A Booming and Lucrative Market for Hackers

20. According to experts, medical identity theft is on the rise because it pays. In black market auctions, complete patient medical records fetch prices higher than credit card numbers. One security expert said that at one auction a patient medical record sold for $251, while credit card records were selling for $0.33.

21. Underground hacker markets are booming. According to an article published in December 2014 by DELL SecureWorks, *Underground Hacker Markets*, the most significant difference between the 2014 underground hacker markets and those of 2013 is that the markets

BADGLEY MULLINS TURNER PLLC
19929 Ballinger Way NE, Suite 200
Shoreline, WA 98155
T: 206-621-6566
F: 206-621-9686

are booming with counterfeit documents to further enable fraud, including new identity kits, passports, utility bills, Social Security cards and drivers licenses. The underground hacker markets are monetizing every piece of data they can steal or buy and are continually adding services so other scammers can successfully carry out online and in person fraud.

22. Statistics maintained by the United States Department of Health and Human Services say there have been 740 major health care breaches affecting twenty-nine million people over the last five years. According to Katherine Keith, a global focus group leader for breach response services at insurer Beazley, which underwrites cyber liability policies, health care companies are attractive targets to hackers because of the wealth of sensitive personal information maintained in their networks. Such information about customers is more valuable on the black market than the credit card information often stolen from retailers. Hence, the combination of Social Security information and a patient's medical history constitutes a valuable commodity to criminals. Stolen medical information can also make false insurance claims.

B. A Critical Need to Secure and Protect Data from Breach in the Healthcare Industry

23. The push to digitized patient health records in hospitals and doctors' offices has also made medical records increasingly vulnerable. According to security experts, moving medical records from paper to electronic form has made patient records more susceptible to breaches, including criminal attack. "'The healthcare industry has become, over the last three years, a much bigger target,'" according to Daniel Nutkas, the Chief Executive of Health Information Trust Alliance, an industry group that works with healthcare organizations to improve their data security.[2] Despite this, healthcare providers have lagged far behind other industries according to experts. "'When we go to a healthcare show and you look at the screens of different systems, it's like we're looking at Windows XP," said Bob Janacek, a co-founder and chief technology officer of DataMotion, an email encryption and health information service

[2] http://www.nytimes.com/2015/02/07/business/data-breach-at-anthem-may-lead-to others.html (last accessed Apr. 8, 2015).

BADGLEY MULLINS TURNER PLLC
19929 Ballinger Way NE, Suite 200
Shoreline, WA 98155
T: 206-621-6566
F: 206-621-9686

provider. "You go to a banking show and they're talking about how to slice a billionth of a second off a transaction to get a competitive edge, it's just totally different.'" *Id.*

24. Healthcare companies, including Premera, were specifically warned by the Federal Bureau of Investigation in 2014 of the increasing threat to them from hackers. About 90% of healthcare organizations have reported that they have had at least one data breach over the last two years, according to a survey of healthcare providers published last year by the Ponemon Institute, a privacy and data protection research firm.

C. Premera's Collection and Storage of Significant Quantities of Sensitive Data

25. Premera fully understood that its customers placed a premium on privacy. Premera provides its customers with a Notice of Privacy Practices.[3] Premera also dedicates a section of its website to explain its privacy and data collection policies.[4]

26. According to Premera, it is "committed to maintaining the confidentiality of your medical and financial information," including customers' names, Social Security numbers, addresses, telephone numbers, account numbers, medical history and claims information. Premera assures the individuals whose data it supposedly secures that it has secured its "electronics systems against unauthorized access" and it further acknowledges that "[u]nder both [HIPPA] and the Gramm-Leach-Bliley Act, Premera Blue Cross must take measures to protect the privacy of your personal information." In addition, Premera represents that it will "protect the privacy of your information even if you no longer maintain coverage through us." Premera's Notice to its customers explains that it collects most personal and health information directly from its insureds while acknowledging that it may collect information from third parties such as employers, other health care providers and state and federal agencies. Premera's Notice further acknowledges that it is required by law to "notify [customers] following a breach of … unsecured personal information." Premera unquestionably knew of the importance that its

[3] *See* Notice of Privacy Practices, available at https://www.premera.com/documents/000160.pdf (last visited Apr. 8, 2015).

[4] *See* https://www.premera.com/wa/visitor/privacy-policy/ (last visited Apr. 8, 2015). The privacy section of Premera's website is substantially similar to the printed Notice of Privacy Practices provided to each Premera customer.

BADGLEY MULLINS TURNER PLLC
19929 Ballinger Way NE, Suite 200
Shoreline, WA 98155
T: 206-621-6566
F: 206-621-9686

customers and others placed on privacy, and its own duty to safeguard the personal information supplied to it and to properly notify victims of any data breach of its systems.

D. Premera did not Adequately Secure Confidential Information or Protect it from Theft

27. Premera had to use every means available to it to protect private and confidential data, including Social Security numbers, from falling into the hands of criminals or hackers. Premera could have converted customers' and employees' confidential and sensitive information into coded strings that were not immediately useful or identifiable to cyber thieves, instead, and no doubt because it did not want to spend the money to do it right, but sacrificing data security on the altar of corporate profits, Plaintiff is informed, believes and hereupon alleges that Premera failed to take that step and many others that would have guarded the confidential information in its possession from attack and theft.

28. Premera was not concerned with protecting its former and current customers from identity theft. Instead, it was more concerned with its financial results and Wall Street's reaction to those results. In that regard, Wall Street has shrugged off data breaches and healthcare providers and non-healthcare providers while viewing such examples of corporate cyber-weaknesses being almost meaningless. Unfortunately, Wall Street's "ho-hum attitude" toward cyber theft, exemplified by the insignificant share price movements upon their announcement, evinces another concern, that companies view corporate security breaches as so frequent and ubiquitous that they have become little more than a routine cost of doing business.

29. "Companies are getting off relatively unscathed," said Paul Stevens, Director of Policy and Advocacy for the Privacy Rights Clearinghouse in San Diego, adding, "they provide some credit monitoring to placate customers, but they have no real incentive to do better."[5] Businesses like Premera harbor a reckless attitude while shunning the steps that must be taken in order to truly achieve cyber security because those steps tend to slow things down and harm productivity.

[5] "Wall Street's reaction to Anthem data breach: ho-hum" http://www.latimes.com/business/la-fi-lazarus-20150206-column.html (last accessed Apr. 8, 2015).

BADGLEY MULLINS TURNER PLLC
19929 Ballinger Way NE, Suite 200
Shoreline, WA 98155
T: 206-621-6566
F: 206-621-9686

E. Confidential Information and Data has Been Breached and Stolen Due to Premera's Misconduct

30. On or about May 5, 2014, hackers infiltrated Premera's Information Technology (IT) system. During the following eight months, hackers gained access to eleven million records of current and former Premera customers and employees, and Blue Cross Blue Shield customers who received medical treatment in Washington or Alaska. For each affected customer, hackers could access the customer's name, date of birth, email address, address, telephone number, Social Security number, member identification number, bank account information, and claims information, including clinical data.

31. Hackers operated inside Premera's systems undetected for nearly nine months until January 29, 2015.

32. Although Premera discovered the breach on January 29, 2015, it did not notify its customers or the public until over six weeks later, on March 17, 2015. Premera disclosed publicly that hackers had breached its cyber security systems and potentially stolen the personal and health information of eleven million current and former customers and employees. Customer records as far back as 2002 were affected by the breach.

33. Premera stated that the breach affected current and former customers of Premera Blue Cross, Premera Blue Cross Blue Shield of Alaska, and Premera's affiliates, including Vivacity, and Connexion Insurance Solutions, Inc. Several days after the breach, LifeWise Health Plan of Oregon announced that 60,000 of its members were compromised by the breach.

34. In addition, Premera acknowledged that the breach affected members of any Blue Cross Blue Shield plan who had received medical treatment in Washington or Alaska. Premera stated "[i]ndividuals who do business with us and provided us with their email address, personal bank account number or Social Security number are also affected."[6]

35. Upon information and belief, hackers could access customers' health information and financial information because Premera did not store such information on separate databases.

[6] Statement of Jeffrey Roe, *available at* http://www.premeraupdate.com/ (last visited Apr. 8, 2015).

BADGLEY MULLINS TURNER PLLC
19929 Ballinger Way NE, Suite 200
Shoreline, WA 98155
T: 206-621-6566
F: 206-621-9686

36. Premera President Jeffrey Roe issued a statement accompanying the Company's public disclosure. In it, he confirmed that attackers "gained unauthorized access to [Premera's] IT systems." Mr. Roe's statement further confirmed that the compromised data included "member name, date of birth, email address, address, telephone number, Social Security number, member identification numbers, bank account information, and claims information, including clinical information." Mr. Roe assured customers that "the security of our members' personal information is a top priority." *Id.*

37. Mr. Roe did not explain why Premera waited over six weeks to notify its customers of the security breach. A statement on its website, however, claims it waited six weeks so it could "block the attack" and "cleanse" its IT systems.[7] Premera has not explained why it could not block the attack and cleanse its IT system while simultaneously notifying its customers that their data was compromised.

38. Around the time that Premera learned of the data breach, Anthem Inc. also discovered that its cyber security system was compromised. Anthem Inc. learned of the breach of its systems on January 27, 2015—two days prior to Premera's discovery. Anthem Inc. publicly disclosed the breach on February 4, 2015. The breach at Anthem Inc. affected eighty million customers, many Blue Cross Blue Shield customers across the United States.[8]

39. Because the Anthem Inc. data breach affected so many Blue Cross Blue Shield customers, Premera Blue Cross customers reasonably wondered whether they too should be concerned. On February 5, 2015, however, Jim Grazko, president of Premera Blue Cross Blue Shield of Alaska, assured the public that the Anthem breach did not affect Premera customers.[9] Although perhaps true, on February 5, 2015, Premera knew its own systems had been breached and its own customers affected by that breach. Premera said nothing.

---

[7] *See* FAQ, available at http://www.premeraupdate.com/faqs/ (last visited Apr. 8, 2015).

[8] *See* "Millions of Anthem Customers Targeted in Cyberattack," New York Times, Reed Abelson & Matthew Goldstein, Feb. 5, 2015, available at http://www.nytimes.com/2015/02/05/business/hackers-breached-data-of- millions-insurer-says.html?_r=0 (last visited Apr. 8, 2015).

[9] *See* "No Signs So Far that Anthem Health Care Data Breach Affects Alaska," Feb. 5, 2015, *available at* http://www.ktuu.com/news/news/no-signs-so-far-that-anthem-health-care-data-breach-affects-alaska/31119336 (last visited Apr. 8, 2015).

BADGLEY MULLINS TURNER PLLC
19929 Ballinger Way NE, Suite 200
Shoreline, WA 98155
T: 206-621-6566
F: 206-621-9686

40. Perhaps more disturbing, Premera was explicitly warned by the federal government that its cyber security systems were vulnerable before the breach occurred in May 2014. On April 18, 2014, the Office of Personnel Management delivered the results of an audit it performed on Premera's IT systems. The audit identified ten areas in which Premera's systems were inadequate and vulnerable to attack.[10]

41. Specifically, the audit found that Premera was not timely implementing critical security patches and other software updates. The audit warned, "Failure to promptly install important updates increases the risk that vulnerabilities will not be remediated and sensitive data could be breached."[11]

42. Auditors determined that several of Premera's servers contained applications so old they were no longer supported by the application's vendor and had known security problems. *Id.*

43. In addition, Premera's servers were insecurely configured, which rendered them more vulnerable to hacking. *Id* at 8.

44. Three weeks after Premera received this audit, its system was compromised. Premera would remain ignorant of the security breach for nearly nine months.

45. In its public disclosure on March 17, 2015, Premera stated that it would notify customers of the breach in a letter sent via U.S. mail. Premera estimated that it would not complete this notification process until April 20, 2015.

46. The Plaintiff received notice of the breach via U.S. Mail in a March 17, 2015 letter from Jeffrey Roe, President and Chief Executive Officer of Premera Blue Cross. In the letter of March 17, 2015, Mr. Roe acknowledged the cyber attack at Premera and acknowledged

[10] *See* "Feds Warned Premera About Security Flaws Before Breach, Seattle Times, Mike Baker," Mar. 18, 2015, available at http://www.seattletimes.com/business/local-business/feds-warned-premera-about-security-flawsbefore-breach/ (last visited Apr. 8, 2015).

[11] U.S. Office of Personnel Management, Office of the Inspector General, Office of Audits, Audit of Information Systems General and Application Controls at Premera Blue Cross 7 (Nov. 28, 2014), https://s3.amazonaws.com/s3.documentcloud.org/documents/1688453/opm-audit.pdf. The Final Audit Report was delivered to Premera on November 28, 2014, but the audit's initial findings were delivered to Premera in April 2014. Premera then had an opportunity to respond before the audit findings became final.

BADGLEY MULLINS TURNER PLLC
19929 Ballinger Way NE, Suite 200
Shoreline, WA 98155
T: 206-621-6566
F: 206-621-9686

that Premera failed to notify the Plaintiff of the cyber attack until March 17, 2015, despite Premera's belief that the hackers' "initial attack occurred on May 5, 2014," and Premera discovered the cyber attack on January 29, 2015.

47. The Plaintiff has tried to guard against any further identity theft relating to their personal information and identity. In that regard, he has or will imminently try to guard against further identity theft. Such steps shall or imminently will include:

a. Filing a report of the breach with the Federal Trade Commission (FTC);

b. Freezing credit reports with each of the three major credit reporting bureaus;

c. The major credit bureaus, however, charge $30 to freeze a credit report by default. This charge can be avoided only if the filer has previously filed a police report. To file a police report, the filer must submit the FTC report number. Upon information and belief, many members of the Class will incur charges freezing their credit report because it is not obvious that the cost is waived only where one has previously filed a police report. Premera has offered no assistance.

d. Further, upon information and belief, the three major credit reporting bureaus maintain websites that are difficult to navigate for the average user and often unclear as to what is provided as a free service and what is not a free service. Upon information and belief, many members of the Class will pay for reporting services that are not needed because they do not understand the process, and Premera has not offered sufficient guidance to navigate this process.

48. Each of these steps requires significant time and individual hardship. The Plaintiff has spent hours attempting to report the data breach. It is often unclear what must be done in order to comprehensively protect oneself. Premera has offered no third-party assistance to help potential victims navigate the reporting process.

BADGLEY MULLINS TURNER PLLC
19929 Ballinger Way NE, Suite 200
Shoreline, WA 98155
T: 206-621-6566
F: 206-621-9686

49. Premera has stated that it has "no evidence to date that [compromised] data has been used inappropriately."[12] Upon information and belief, however, it is likely that customer files are now on sale on the black market or will be soon.

50. Premera has also offered two years of free credit monitoring to affected customers. For reasons explained in more detail below, credit monitoring is entirely inadequate given the breadth of information stolen. Credit monitoring does little to protect against tax or insurance fraud, or to prevent imposters from obtaining medical treatment or prescription drugs fraudulently. Premera offers its customers nothing to guard against these reasonably foreseeable threats.

F. The Ongoing Harm Arising from the Premera Cyber Attack and Data Breach

51. The compromised data leaves Premera customers and victims especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more. These types of data breaches can cause numerous adverse consequences because the hackers and the parties to whom such information is sold can commit fraud that lasts over a long period. This is the kind of identity theft that is qualitatively and quantitatively different than losing one's credit card. Social Security numbers are among the worst personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

52. Social Security administration has warned that identity thieves can use an individual's Social Security number and good credit score to apply for additional credit lines. This fraud can go undetected until debt collection calls commence months or even years later.[13]

53. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. This may cause conflict or suspicion

[12] *See* FAQ, available at http://www.premeraupdate.com/faqs/ (last visited Apr. 8, 2015).

[13] Social Security Administration, "Identity Theft and Your Social Security Number," http://www.ssa.gov/pubs/EN05-10064.pdf (last visited Apr. 8, 2015).

BADGLEY MULLINS TURNER PLLC
19929 Ballinger Way NE, Suite 200
Shoreline, WA 98155
T: 206-621-6566
F: 206-621-9686

between an employer and employee, and may trigger investigations of the employee that require time and expense to defend. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected. It can take months or years, and significant expense to the victim, to correct the fraud with the IRS.

54. The incidence of fraudulent tax filings has increased dramatically over the past years. The IRS paid an estimated $5.2 billion in tax refunds obtained from identity theft in 2013, while it prevented an additional $24.2 billion in fraudulent transfers the same year.[14]

55. Also, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Preventive action to defend against the possibility of misuse is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

56. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[15]

57. Another danger, according to the publisher of Privacy Journal, Robert Ellis Smith, is that thieves use stolen Social Security numbers to obtain medical care in someone else's name. *Id.*

58. Medical identity fraud affected 2.3 million people in 2014—an increase of 21% over the previous year. A study by the Ponemon Institute concluded that victims of such fraud spend an average of $13,500 to resolve problems stemming from medical identity theft.[16]

---

[14] "FBI Probes Rash of Fraudulent State Tax Returns Filed Through Turbo Tax," Los Angeles Times, Shan Li, Feb. 11, 2015, available at http://www.latimes.com/business/la-fi-turbotax-fbi-20150212-story.html (last visited Apr. 8, 2015).

[15] "Victims of Social Security Number Theft Find It's Hard to Bounce Back," NPR, Brian Naylor, Feb. 9, 2015, available at http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worryingabout-identity-theft (last visited Apr. 8, 2015).

[16] Ponemon Institute LLC, "Fifth Annual Study on Medical Identity Theft" (Feb. 2015), available at http://assets.fiercemarkets.com/public/healthit/ponemonmedidtheft2015.pdf (last visited Apr. 8, 2015).

BADGLEY MULLINS TURNER PLLC
19929 Ballinger Way NE, Suite 200
Shoreline, WA 98155
T: 206-621-6566
F: 206-621-9686

59. Fraudulent medical treatment can have non-financial impacts as well. Deborah Peel, executive director of Patient Privacy Rights, has described scenarios in which an individual may be given an improper blood type or administered medicines because his or her medical records contain information supplied by an individual obtaining treatment under a false name.[17]

60. In the Premera hack, customer clinical information was compromised. This means any information in an individual's medical records is subject to disclosure or, worse, medical blackmail.

61. The Ponemon Institute study concluded that a victim of medical identity theft rarely learns of the fraudulent treatment for three months. To guard against medical identity fraud, cyber security experts suggest that individuals routinely obtain the most recent copy of their medical records and inspect them for discrepancies. Premera's proposed customer solutions do nothing to address the problem of medical identity theft, and Premera has done nothing to advise its customers how to obtain and inspect their medical records for fraud to comport with best practices identified by security experts.

62. The victims of the Premera breach are also now at heightened risk of health insurance discrimination. Stolen medical and clinical information may be improperly disclosed for use to discriminate in the provision of healthcare to insureds and prospective insureds. Individuals risk denial of coverage, improper "redlining," and denial or difficulty obtaining disability or employment benefits because information was improperly disclosed to a provider. This risk is pervasive and widespread. Most states maintain government agencies that investigate and combat health insurance discrimination, as does the Office for Civil Rights in the Department of Health and Human Services.

[17] *See* "2015 is Already the Year of the Health-Care Hack—and It's Only Going to Get Worse," Wash. Post, Andrea Peterson, Mar. 20, 2015, available at http://www.washingtonpost.com/blogs/the-switch/wp/2015/03/20/2015-is-already-the-year-of-the-health-care-hack-and-its-only-going-to-get-worse/ (last visited Apr. 8, 2015).

BADGLEY MULLINS TURNER PLLC
19929 Ballinger Way NE, Suite 200
Shoreline, WA 98155
T: 206-621-6566
F: 206-621-9686

63. The danger of identity theft is compounded when a minor's Social Security number and personal information is compromised. Whereas adults can periodically monitor their own credit reports, minors typically have no credit to monitor. It can be difficult to safeguard against fraud. Thieves who steal a minor's identity may use it for years before the crime is discovered.

64. Premera is offering a "family secure service" through Experian for customers with minor children. This service provides monthly monitoring to ascertain whether a minor's Social Security number has been used to access credit. This service, while a step in the right direction, is inadequate; it permits fraudsters a thirty-day window in which to commit fraud without fear of detection via monitoring.

65. The personal information compromised in the Premera breach is more valuable than the credit card information compromised in the large retailer data breaches at Target and Home Depot. Victims affected by the retailer breaches could avoid much of the potential for future harm by cancelling credit or debit cards and obtaining replacements. The information compromised in the Premera breach is difficult, if not impossible, to change—Social Security number, name, date of birth, clinical information, etc.

66. These data, as one would expect, demand a much higher price on the black market. Martin Walter, senior director at cyber security firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[18]

67. This estimate may be low. A recent PricewaterhouseCoopers report stated that an identity theft kit containing health insurance credentials can be worth up to $1,000 on the black market, while stolen credit cards may go for $1 each.

68. Premera has announced that it will offer free credit monitoring services for two years. As security blogger Brian Krebs has explained, however, "the sad truth is that most

[18] "Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers," IT World, Tim Greene, Feb. 6, 2015, *available at* http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for10x-price-of-stolen-credit-card-numbers.html (last visited Apr. 8, 2015).

BADGLEY MULLINS TURNER PLLC
19929 Ballinger Way NE, Suite 200
Shoreline, WA 98155
T: 206-621-6566
F: 206-621-9686

services offer little in the way of real preventive protection against the fastest-growing crime in America [identity theft]."[19] Credit monitoring services may inform individuals of fraud after the fact, but do little to thwart fraud from occurring in the first instance. These services do little to defend against medical identity theft or misuse of Social Security numbers for non-financial fraud.

69. The implications of the Premera data breach are serious. But these implications were known ex ante. Premera should have—and could have—done more to fulfill its duty to safeguard the data with which its customers entrusted it. And it could—and should—do more to protect its customers now that a breach has occurred.

V. CLASS ACTION ALLEGATIONS

70. Plaintiff sues as a Class action on his own behalf and on behalf of all other persons similarly situated as members of the proposed Class under Federal Rules of Civil Procedure 23(a) and (b)(3) and/or (b)(2). This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of those provisions.

71. The proposed Nationwide Class is defined as:

Nationwide Class

All persons in the United States who were insured by Premera and/or its affiliates for any period of time beginning in 2002 until January 29, 2015, and all persons in the United States who were not Premera insureds but who are or were Blue Cross Blue Shield customers and who received medical treatment in Washington or Alaska between 2002 and January 29, 2015.

72. Plaintiff also sues on behalf of a Premera Treatment Subclass, defined as:

Premera Treatment Subclass

All persons who were not insured by Premera and/or its affiliates for any period of time beginning in 2002 until January 29, 2015, but who were insured by Blue Cross Blue Shield and received medical treatment in Washington or Alaska between 2002 and January 29, 2015.

[19] Brian Krebs, "Are Credit Monitoring Services Worth It?," Krebs on Security, Mar. 19, 2014, http://krebsonsecurity.com/2014/03/are-credit-monitoring-services-worth-it/ (last visited Apr. 8, 2015).

BADGLEY MULLINS TURNER PLLC
19929 Ballinger Way NE, Suite 200
Shoreline, WA 98155
T: 206-621-6566
F: 206-621-9686

73. Excluded from the Classes and Subclass are: (1) Defendant, any entity or division in which Defendant has a controlling interest, and its legal representatives, officers, directors, assigns, and successors; (2) the Judge to whom this case is assigned and the Judge's staff; and (3) governmental entities. Plaintiff reserves the right to amend the Class definition if discovery and further investigation reveal that the Class should be expanded, divided into subclasses or modified in any other way.

A. Numerosity and Ascertainability

74. Although the exact number of Class members is uncertain and can be ascertained only through discovery, the number is great enough such that joinder is impracticable. The disposition of the claims of these Class members in a single action will provide substantial benefits to all parties and to the Court. Class members are readily identifiable from information and records in Premera's possession, custody, or control.

B. Typicality

75. Plaintiff's claims are typical of the claims of the Class in that Plaintiff, like all Class members, entrusted personal and health information to Premera for healthcare services or treatment. Plaintiff, like all Class members, has been damaged by Premera's conduct in that his personal and health information, including his Social Security number and clinical information, has been compromised by Premera's failure to fulfill its duties under the law. Further, the factual bases of Premera's misconduct are common to all Class members and represent a common thread of misconduct resulting in injury to all Class members.

C. Adequate Representation

76. Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel with substantial experience in prosecuting consumer and data breach Class actions, and therefore Plaintiff's counsel is adequate under Rule 23.

77. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the Class and have the financial resources to do so. Neither Plaintiff nor his counsel has interests adverse to those of the Class.

BADGLEY MULLINS TURNER PLLC
19929 Ballinger Way NE, Suite 200
Shoreline, WA 98155
T: 206-621-6566
F: 206-621-9686

D. Predominance of Common Issues

78. There are numerous questions of law and fact common to Plaintiff and the Class members that predominate over any question affecting only individual Class members. The answers to these common questions will advance resolution as to all Class members. These common legal and factual issues include:

a. Whether Premera owed a duty to Plaintiff and members of the Class to take reasonable measures to safeguard their personal information;

b. Whether Premera knew or should have known that its cyber security systems were vulnerable to attack;

c. Whether Premera's breach of a legal duty caused its cyber security systems to be compromised, resulting in the loss and/or potential loss of eleven million member files;

d. Whether Premera owed a duty to Plaintiff and members of the Class to provide timely and adequate notice of the Premera data breach and the risks posed, and whether Premera's notice was timely;

e. Whether Premera violated Washington state law requiring notice within the "most expedient time possible" when a data breach occurs; and

f. Whether Plaintiff and Class members may recover actual damages, statutory damages, and/or punitive damages.

E. Superiority

79. Plaintiff and Class members have all suffered and will continue to suffer harm and damages because of Premera's unlawful and wrongful conduct. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy.

80. Absent a Class action, most Class members would likely find the cost of litigating their claims prohibitively high and would therefore have no effective remedy at law. Further, without Class litigation, Class members will continue to incur damages and Premera is likely to repeat its misconduct.

BADGLEY MULLINS TURNER PLLC
19929 Ballinger Way NE, Suite 200
Shoreline, WA 98155
T: 206-621-6566
F: 206-621-9686

81. Class treatment of common questions of law and fact is also a superior method to multiple individual actions or piecemeal litigation in that Class treatment will conserve the resources of the courts and the litigants, and will promote consistency and efficiency of adjudication.

VI. CAUSES OF ACTION

FIRST CLAIM FOR RELIEF
Negligence
(Asserted on Behalf of the Nationwide Class)

82. Plaintiff incorporates by reference the allegations in the preceding paragraphs of this Complaint.

83. Plaintiff brings this Claim on behalf of the Nationwide Class under Washington law.

84. Plaintiff brings this Claim on behalf of the Washington Class under Washington state law.

85. Premera required Plaintiff and Class members to submit non-public personal and health information to acquire coverage under a health insurance policy and/or receive treatment in the Blue Cross Blue Shield network while in Washington or Alaska. Premera collected and stored this data. It therefore assumed a duty of care to use reasonable means to secure and safeguard this personal and health information, to prevent disclosure of the information, and to guard the information from theft. Premera's duty included a responsibility to implement a process by which it could detect a breach of its security systems in a reasonably expeditious period of time.

86. Premera's duty arises from the common law, and the principles embodied in Washington state law, Article I, Section 7 of the Washington Constitution, and HIPAA.

87. Premera breached its duty of care by failing to secure and safeguard the personal and health information of Plaintiff and the Class. Premera negligently maintained systems it knew were vulnerable to a security breach. It knew these vulnerabilities, yet failed to rectify them. Further, Premera negligently stored financial and health information unencrypted on the

BADGLEY MULLINS TURNER PLLC
19929 Ballinger Way NE, Suite 200
Shoreline, WA 98155
T: 206-621-6566
F: 206-621-9686

same database, making it more likely a breach would net a greater (and more dangerous) breadth of personal information.

88. Given the risks associated with data theft, Premera also assumed a duty of care to promptly and fully notify and inform its customers should their personal information be compromised and/or stolen.

89. Premera breached this duty of care when it unreasonably waited over six weeks to notify the Class that its security systems had been breached. Premera learned of the breach on January 29, 2015, yet said nothing to notify those affected for over six weeks. Premera even assured its customers they had nothing to fear, emphasizing that the breach at Anthem Inc. in early February 2015 did not affect Premera customers. While this is true, Premera offered these assurances knowing full well that its customers' data was compromised by an independent breach that potentially affected an even greater breadth of information than the breach experienced at Anthem Inc. Premera continues to breach this duty of care, by failing to share crucial information with Plaintiff and the Class.

90. Plaintiff and the Class have suffered harm because of Premera's breach. The personal and health information of Plaintiff and the Class have been exposed, subjecting each member of the Class to identity theft, credit and bank fraud, Social Security fraud, tax fraud, medical identity fraud, and myriad other varieties of identity fraud.

91. Plaintiff and the Class has suffered monetary damages and will continue to be injured and incur damages both to protect themselves and to remedy acts of fraudulent activity. Plaintiff and the Class have suffered and/or are reasonably likely to suffer theft of personal and health information; costs associated with prevention, detection, and mitigation of identity theft and/or fraud; costs associated with time spent and productivity loss resulting from addressing the consequences of fraud in any of its myriad forms; and damages from the unconsented exposure of personal and health information due to this breach.

SECOND CLAIM FOR RELIEF
Negligence Per Se
(Asserted on Behalf of the Nationwide Class)

BADGLEY MULLINS TURNER PLLC
19929 Ballinger Way NE, Suite 200
Shoreline, WA 98155
T: 206-621-6566
F: 206-621-9686

92. Plaintiff incorporates by reference the allegations in the preceding paragraphs of this Complaint.

93. Plaintiff brings this Claim on behalf of the Nationwide Class under Washington law.

94. Plaintiff brings this Claim on behalf of the Washington Class.

95. Under HIPPA, Premera had a duty to secure and safeguard the personal information of its customers. Premera acknowledged this duty to its customers in its Notice of Privacy Practices, and warranted that it would comport with its duties under HIPAA.

96. Premera violated HIPAA by failing to secure and safeguard the personal information entrusted to it by Plaintiff and the Class. Further, Premera failed to implement protections against "reasonably anticipated threats," 45 C.F.R. § 164.306, and failed to encrypt customer data or implement an equivalent alternative measure and document the reason or reasons that encryption was not reasonable. *Id.* § 164.312.

97. Premera's failure to comply with HIPAA and regulations promulgated there to constitutes negligence per se.

98. Because of Premera's negligence per se, Plaintiff and the Class have suffered monetary damages and will continue to be injured and incur damages both to protect themselves and to remedy acts of fraudulent activity. Plaintiff and the Class have suffered and/or are reasonably likely to suffer theft of personal and health information; costs associated with prevention, detection, and mitigation of identity theft and/or fraud; costs associated with time spent and productivity loss resulting from addressing the consequences of fraud in any of its myriad forms; and damages from the unconsented exposure of personal and health information due to this breach.

THIRD CLAIM FOR RELIEF
Violation of Breach of Fiduciary Duty
(Asserted on Behalf of the Nationwide Class)

99. Plaintiff incorporates by reference the allegations in the preceding paragraphs of this Complaint.

BADGLEY MULLINS TURNER PLLC
19929 Ballinger Way NE, Suite 200
Shoreline, WA 98155
T: 206-621-6566
F: 206-621-9686

100. Plaintiff brings this Claim on behalf of the Nationwide Class under Washington law.

101. Premera collected and stored highly personal and private information, including health information, belonging to Plaintiff and members of the Class. Because this information is of a heightened sensitivity and importance, it receives special protection under federal law. HIPAA protects all "individually identifiable health information," and individual identifiers such as Social Security numbers and medical identification numbers. See, e.g., 45 C.F.R. § 160.103. Also, HIPAA imposes heightened duties on entities like Premera that collect and store such information, subjecting them to a range of penalties when protected health information is wrongfully disclosed. *See*, e.g., 42 U.S.C. §§ 1320d-5, 1320d-6.

102. The protected health information also receives heightened protection under Washington state law. The Revised Code of Washington applies special duties upon a business that stores "personal information," including Social Security numbers, credit, and banking information. See RCW 19.255.010. Where a business suffers a data breach exposing such information, the law places heightened duties of disclosure on that business. *Id*.

103. By its collection of highly personal information, including health information, and the warranties made in its Notice of Privacy Practices, a fiduciary relationship arose between Premera and the Class members that is actionable at law.

104. By this fiduciary relationship, Premera owed Plaintiff and members of the Class a fiduciary duty to safeguard the personal and health information it collected and stored; to warn Plaintiff and the Class when it learned that the security of the collected data may be vulnerable; and to immediately and fully notify Plaintiff and the Class when it knew that its cyber security systems had been breached. This duty required Premera to ensure that the interests of Plaintiff and the Class would be adequately cared for, both before and after the security breach. By its duty, Premera owes Plaintiff and the Class assistance in protecting themselves now that a breach has occurred, not just from financial fraud, but also from medical identity fraud, health insurance discrimination, tax fraud, and other forms of identity fraud described.

BADGLEY MULLINS TURNER PLLC
19929 Ballinger Way NE, Suite 200
Shoreline, WA 98155
T: 206-621-6566
F: 206-621-9686

105. If the Court finds this Claim may not be raised on behalf of the Nationwide Class, Plaintiff and the Class bring this Claim on behalf of the Washington State Class under Washington law and, separately, on behalf of the Premera Treatment Subclass under the law of Class members' respective domicile.

106. Because of Premera's breach of its fiduciary duties, Plaintiff and the Class have suffered actual damages, and prospective damages reasonably likely to arise. Premera has tried to protect the Class from these reasonably likely prospective damages, and Plaintiff and the Class therefore request equitable and/or injunctive relief to require Premera to prevent the forms of identity fraud alleged.

PRAYER FOR RELIEF

Plaintiff, on behalf of himself and all others similarly situated, request the Court to enter judgment against Defendant:

A. An order certifying the proposed Class designating Plaintiff as the named representative of the Class, and designating the undersigned as Class Counsel;

B. An order awarding Plaintiff and the Class relief, including actual and statutory damages, and equitable and/or injunctive relief as requested;

C. An injunction ordering Premera to immediately notify each individual whose personal information was compromised and/or an order awarding Plaintiff and the Class preliminary or other equitable or declaratory relief as may be appropriate by way of applicable state or federal law and as requested;

D. Any additional orders or judgments as may be necessary to prevent further unlawful practices and to restore to any person in interest any money or property that may have been acquired with the violations;

E. An award of attorneys' fees and costs, as provided by law;

F. An award of pre-judgment and post-judgment interest, as provided by law;

G. Leave to amend this Complaint to conform to the evidence produced ; and

H. Any other favorable relief as may be available and appropriate under law or at equity.

BADGLEY MULLINS TURNER PLLC
19929 Ballinger Way NE, Suite 200
Shoreline, WA 98155
T: 206-621-6566
F: 206-621-9686

JURY DEMAND

Under Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of all issues so triable of right.

RESPECTFULLY SUBMITTED AND DATED this 14th day of April, 2015.

DATED: April 14, 2015

Respectfully submitted,

BADGLEY MULLINS TURNER PLLC
DUNCAN C. TURNER

/s/ DUNCAN C. TURNER
DUNCAN C. TURNER

19929 Ballinger Way NE, Suite 200
Shoreline, WA 98155
Telephone: (206) 621-6566
Facsimile: (206) 621-9686

John G. Emerson
EMERSON POYNTER LLP
830 Apollo Lane
Houston, TX 77058-2610
Telephone: (281) 488-8854
Facsimile: (281) 488-8867
Email: jemerson@emersonpoynter.com
(pending pro hac vice)

Scott E. Poynter
Will T. Crowder
EMERSON POYNTER LLP
1301 Scott Street
Little Rock, AR 72202
Telephone: (501) 907-2555
Facsimile: (501) 907-2556
Email: scott@emersonpoynter.com
Email: wcrowder@emersonpoynter.com
(pending pro hac vice)
Attorneys for Plaintiff, the Proposed Nationwide Class and the Proposed Premera Treatment Subclass